**Luka w zabezpieczeniach może pozwolić hakerom na dostęp do aplikacji iOS.**

**Niedawno wykryta luka w aplikacjach na iOS może umożliwić hakerom uruchomienie złośliwego kodu w zaatakowanych aplikacjach, pod warunkiem, że urządzenie jest podłączone do sieci Wi-Fi kontrolowanej przez atakującego.**

Liczba potencjalnie zagrożonych aplikacji szacowana jest na około 10 procent aplikacji dostępnych dla iOS.

Zespół Jailbreaking, który zgłosił tę lukę, nie opublikował jeszcze żadnych szczegółów technicznych na temat tego, w jaki sposób można wykorzystać błąd oprogramowania. Udostępniono natomiast film z potwierdzeniem jego istnienia.

"Podczas audytu aplikacji iOS, Pangu Lab zauważył wspólny błąd programowania, który prowadzi do poważnych konsekwencji, takich jak nadpisanie danych, a nawet uruchomienie złośliwego kodu w kontekście aplikacji podlegających usterce", czytamy na stronie internetowej ZipperDown. "Niespodziewanie odkryliśmy, że 10% aplikacji na iOS mogą być podatne na te same lub podobne problemy."

„Przekonanie o braku istnienia złośliwego oprogramowania na system iOS to już dawno mit”, komentuje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken, „jeszcze kilka lat temu Firma Apple uważała wręcz, że na ich mobilny system wirusów nie ma wcale. Co prawda odsetek malware jest dużo mniejszy niż liczba malware stworzona na Androida. Jednak rosnąca liczba infekcji na platformę iOS powinna nam dać do myślenia” – dodaje.

Spekulacje, że luka w oprogramowaniu może leżeć w powszechnie używanym narzędziu o nazwie ZipArchive, nie zostały jeszcze potwierdzone przez zespół Pangu, który twierdzi, że stara się powstrzymać hakerów przed wykorzystywaniem błędu. Zespół opublikował jednak listę potencjalnie zainfekowanych aplikacji na iOS. Wśród nich znajdują się między innymi Instagram, Pandora, Dropbox oraz Amazon.

"Ze względu na dużą liczbę potencjalnie dotkniętych aplikacji, nie możemy dokładnie zweryfikować wszystkich wyników. Dla bezpieczeństwa użytkowników końcowych, szczegóły o aplikacji ZipperDown nie są na razie dostępne publicznie."

Ponieważ atak opiera się na połączeniu do sieci WiFi, która jest kontrolowana przez atakującego, programiści chcą naprawić zaistniały błąd jak najszybciej. Jednak firma Apple jeszcze oficjalnie nie potwierdziła luki w zabezpieczeniach i nie publikuje wskazówek, co deweloperzy muszą zrobić, aby załatać powstałe dziury.

Ci sami badacze zauważyli, że błąd może wpłynąć również na aplikacje na Androida, ponieważ wiele popularnych aplikacji na Androida ma tę samą lukę w zakresie programowania.